



UNITED STATES MARINE CORPS
MARINE CORPS SYSTEMS COMMAND
2200 LESTER STREET
QUANTICO, VIRGINIA 22134-5010

IN REPLY REFER TO:
5720
DON-USMC-2019-010271
9 Mar 20

Sent Via Email to: matnormal@cisco.com

CISCO
Mr. Matt Norman

Dear Mr. Norman:

SUBJECT: SUBMITTER NOTICE RE: FREEDOM OF INFORMATION ACT (FOIA)
REQUEST DON-USMC-2019-010271

The Marine Corps received a request for information under the Freedom of Information Act ("FOIA") and, after conducting a search, we determined that the enclosed records are responsive to the request and must be released unless exempt from disclosure. The purpose of this letter is to provide you with the opportunity to review these records and explain whether you think some or all of the information contained therein is protected from disclosure pursuant to FOIA Exemption 4 (5 U.S.C. § 552(b)(4)). In general, Exemption 4 provides for the withholding of (a) trade secrets and (b) commercial or financial information that is privileged or confidential.

If you think some or all of the information in the enclosed records is exempt from disclosure pursuant to Exemption 4, please respond in writing within 10 working days of the date of this letter and provide the following:

1. Identify the specific information that you think is exempt because it is either (a) a trade secret or (b) confidential commercial or financial information by marking it for redaction with a **yellow highlighter (do not "black out" or obscure the text)**. If you think an entire record is exempt, you can just state that.
2. With respect to any information that you think is exempt because it is a trade secret, please provide a detailed explanation as to why. General assertions without explanations are insufficient.
3. With respect to the information that you think is exempt because it is confidential commercial or financial information, please:

9 Mar 20


a. Advise whether the information is customarily and actually kept private or closely held by your company. If the information is of a type that is typically released to investors, shareholders, the press, or made public in connection with a regulatory filing, then the information is not exempt pursuant to Exemption 4; and

b. Explain whether you or your company received an assurance of confidentiality from the Marine Corps and the basis of that belief (i.e., the circumstances under which that assurance was provided). If you have a non-disclosure agreement, written statement, or other document from the Marine Corps providing the assurance of confidentiality, please provide a copy with your response.

Please respond with the information requested above no later than 10 business days from the date of this letter. If we do not receive your written response by that deadline, we will assume that you have no objection to the full release of the enclosed records, and the release determination will be based solely on the Marine Corps' review.

If you have any questions regarding this matter, you may call me at 703-432-3934 or email me at bobbie.cave@usmc.mil.

Sincerely,


for Lisa L. Baker
Counsel

USMC | Cisco Joint Level Services Agreement

**Marine Corps Systems Command
(MARCORSYSCOM)**

MITC-West Camp Pendleton

Asset Lifecycle Analysis

DON 95

May 2018

Version 2.0

Prepared by Cisco Services

UNCLASSIFIED//FOUO

Cisco Services

13635 Dulles Technology Drive

Herndon VA 20171

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of the UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

Xremote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCDE, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0105R)

INTELLECTUAL PROPERTY RIGHTS:

THIS DOCUMENT CONTAINS VALUABLE TRADE SECRETS AND CONFIDENTIAL INFORMATION OF CISCO SYSTEMS, INC. AND ITS SUPPLIERS, AND SHALL NOT BE DISCLOSED TO ANY PERSON, ORGANIZATION, OR ENTITY UNLESS SUCH DISCLOSURE IS SUBJECT TO THE PROVISIONS OF A WRITTEN NON-DISCLOSURE AND PROPRIETARY RIGHTS AGREEMENT OR INTELLECTUAL PROPERTY LICENSE AGREEMENT APPROVED BY CISCO SYSTEMS, INC. THE DISTRIBUTION OF THIS DOCUMENT DOES NOT GRANT ANY LICENSE IN OR RIGHTS, IN WHOLE OR IN PART, TO THE CONTENT, THE PRODUCT(S), TECHNOLOGY OF INTELLECTUAL PROPERTY DESCRIBED HEREIN.

Asset Lifecycle Analysis for the MITC-West USMC

Copyright © 2001-18, Cisco Systems, Inc.

All rights reserved.

COMMERCIAL IN CONFIDENCE

A PRINTED COPY OF THIS DOCUMENT IS CONSIDERED UNCONTROLLED

Revision History

Date	Version	Change	Responsible Person
09APR18	1.0	Initial Draft	(b) (6)
18APR18	1.1	Second Draft	
24APR18	1.2	Technical Edit//Review	
25APR18	1.3	Minor Update	
25APR18	1.3a	Minor Update	
30APR18	1.4	USMC Feedback Update	
01MAY18	1.5	RED Team Review Update	
02MAY18	2.0	Final Release	

Contents

1.	Introduction.....	1
1.1.	Document Organization.....	1
1.2.	References.....	2
2.	Executive Summary.....	3
3.	Technical Summary	7
3.1.	Introductory Comments	7
3.2.	Assessment Process	7
3.3.	Summary Findings.....	8
4.	Assessment Detail.....	9
4.1.	Hardware Resiliency.....	9
4.1.1.	Recommendations.....	9
4.1.2.	General Hardware Information Observations	10
4.1.3.	Modularity Observations	19
4.1.4.	Scalability Observations	19
4.1.5.	Field Notices	25
4.1.6.	Hardware Replacement and Refresh Strategy	25
4.2.	Software Resiliency	26
4.2.1.	Recommendations:.....	26
4.2.2.	Software Release Management Observations.....	27
4.2.3.	Software Security Advisories Observations	27
4.2.4.	Software Lifecycle Management Observations	29
4.2.5.	Software Analysis	29
5.	USMC and Cisco Participants	44
5.1.	USMC Team	44
5.2.	Cisco Team	45
	Appendix A – Acronyms	46
	Appendix B – LDoS Summaries by Year 2018-2023	50
	LDoS Chassis Summary – (b) (3) (b) (4)	50
	LDoS Chassis Summary (b) (3) (b) (4)	51

LDoS Chassis Summary – (b) (3), (b) (4)	51
LDoS Chassis Summary – (b) (3), (b) (4)	51
LDoS Chassis Summary – (b) (3), (b) (4)	52
LDoS Modules Summary – (b) (3), (b) (4)	52
LDoS Modules Summary – (b) (3), (b) (4)	53
LDoS Modules Summary – (b) (3), (b) (4)	54
LDoS Modules Summary – (b) (3), (b) (4)	54
LDoS Modules Summary – (b) (3), (b) (4)	55
LDoS Modules Summary – (b) (3), (b) (4)	55
Appendix C – Cisco Security Advisories	56
Appendix D – LDoS Now Chassis	60

Figures

Figure 1: Global Chassis Diversity	11
Figure 2: Global Card/Module Diversity Summary	11
Figure 3: Global Fan Tray Diversity Summary	12
Figure 4: Global Power Supply Diversity Summary	12
Figure 5: Router Chassis Diversity Detailed Summary	13
Figure 6: Router Card/Module Diversity Detailed Summary	13
Figure 7: Router FAN Tray Diversity Detailed Summary	14
Figure 8: Router Power Supply Diversity Detailed Summary	14
Figure 9: LAN Switch Chassis Diversity Detailed Summary	15
Figure 10: LAN Switch Hardware Card/Module Detailed Summary	16
Figure 11: LAN Switch FAN Tray Diversity Detailed Summary	17
Figure 12: LAN Switch Power Supply Diversity Detailed Summary	18
Figure 13: Transceiver Module Diversity Detailed Summary	19
Figure 14: Current Hardware EoS Sale Summary	21
Figure 15: LDoS Summary by Year – Chassis	21
Figure 16: LDoS Summary by Year – Cards/Modules	22
Figure 17: LDoS (b) (3), (b) (4)	23

Figure 18: LDoS	(b) (3), (b) (4)	24
Figure 19: Global IOS Software Diversity Summary		30
Figure 20: Global Router IOS Software Diversity Summary		31
Figure 21: Cisco	(b) (3), (b) (4)	31
Figure 22: Cisco	(b) (3), (b) (4)	32
Figure 23: Cisco	(b) (3), (b) (4)	32
Figure 24: Cisco	(b) (3), (b) (4)	33
Figure 25: Cisco	(b) (3), (b) (4)	33
Figure 26: Global Switch IOS Software Diversity Summary		34
Figure 27: Cisco	(b) (3), (b) (4)	34
Figure 28: Cisco	(b) (3), (b) (4)	35
Figure 29: Cisco	(b) (3), (b) (4)	36
Figure 30: Cisco	(b) (3), (b) (4)	36
Figure 31: Cisco	(b) (3), (b) (4)	37
Figure 32: Cisco	(b) (3), (b) (4)	37
Figure 33: Cisco	(b) (3), (b) (4)	38
Figure 34: Cisco	(b) (3), (b) (4)	38
Figure 35: Cisco	(b) (3), (b) (4)	39
Figure 36: Cisco	(b) (3), (b) (4)	40
Figure 37: Cisco	(b) (3), (b) (4)	40
Figure 38: Cisco	(b) (3), (b) (4)	41
Figure 39: Cisco	(b) (3), (b) (4)	42
Figure 40: Cisco	(b) (3), (b) (4)	42
Figure 41: Cisco	(b) (3), (b) (4)	43
Figure 42: LDoS Chassis Summary –	(b) (3), (b) (4)	50
Figure 43: LDoS Chassis Summary –	(b) (3), (b) (4)	51
Figure 44: LDoS Chassis Summary –	(b) (3), (b) (4)	51
Figure 45: LDoS Chassis Summary –	(b) (3), (b) (4)	51
Figure 46: LDoS Chassis Summary –	(b) (3), (b) (4)	52
Figure 47: LDoS Chassis Summary –	(b) (3), (b) (4)	52
Figure 48: LDoS Modules Summary –	(b) (3), (b) (4)	52
Figure 49: LDoS Modules Summary –	(b) (3), (b) (4)	53
Figure 50: LDoS Modules Summary –	(b) (3), (b) (4)	54

Figure 51: LDoS Modules Summary –	(b) (3), (b) (4)	54
Figure 52: LDoS Modules Summary –	(b) (3), (b) (4)	55
Figure 53: LDoS Modules Summary –	(b) (3), (b) (4)	55

Tables

Table 1: Maturity Level Color Coding	7
Table 2: Assessment Overview Findings.....	8
Table 3: Typical EoX Milestone Overview	20
Table 4: Milestone Alert Acronyms	30

1. Introduction

The Cisco Systems Advanced Services Asset Lifecycle Analysis (ALA) seeks to identify gaps in network design practices between the customer processes and Cisco-identified industry leading practices. The Cisco Advanced Services Team assists customers in attaining a higher level of network availability through identification of these gaps and recommendations to address them.

The ALA is an evaluation of a Cisco infrastructure assets environment. The analysis is focused on the lifecycles of both hardware assets (e.g. chassis and modules) as well as the software lifecycles of deployed software trains running on those assets in the network.

For the purposes of brevity, the US Marine Corps team will be referenced with the acronym (USMC) throughout this document.

1.1. Document Organization

This ASSET LIFECYCLE ANALYSIS (ALA) includes the following sections:

- Section 2: [Executive Summary](#) – provides a business overview of the network and key challenges based on business objectives.
- Section 3: [Technical Summary](#) – provides a technical resiliency rating based on identified leading practices and summary recommendations.
- Section 4: [Assessment Detail](#) – identifies the leading practices and provides detailed findings and recommendations for each focus area evaluated in the report.
- Section 5: [USMC and Cisco Participants](#) – list the personnel involved in the (ALA).
- Appendixes

1.2. References

This ALA includes the following references:

- Cisco IOS & NX-OS Software Reference Guides -
<http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html>

Cisco Validated Design Program

- Design Zone for Campus -
<http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-campus/index.html#~validate>
- Cisco Validated Design Program:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns741/networking_solutions_products_genericcontent0900aecd80601e22.html

Cisco DocWiki

- Internetworking Technology Handbook -
http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook

Cisco High Availability Design Guides

- High Availability Technology White Papers -
<http://www.cisco.com/c/en/us/tech/availability/high-availability/tech-white-papers-list.html>
- Cisco IOS Management for High Availability Networking: Best Practices White Paper -
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Cisco Guide to Harden Cisco IOS Devices -
<http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>
- Campus Network for High Availability Design Guide -
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1107057
- Campus and Branch Network Design for BYOD -
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Network_Design.html

2. Executive Summary

The Asset Lifecycle Analysis was performed through on-site collection and analysis of targeted MITC-West USMC network assets. The recommendations provided in this assessment are the result of an analysis of MITC-West USMC network asset's current-state, compared to Cisco databases and software recommendations.

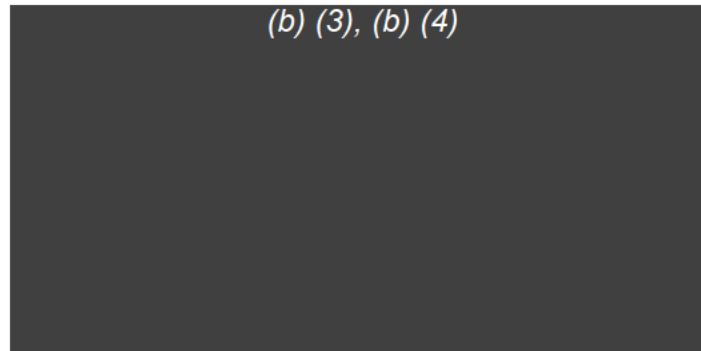
The primary business driver for USMC is to provide a highly available network for NIPR network users with Cisco supported hardware and software.

Hardware Resiliency – (b) (3), (b) (4).

The MITC-West team maintains moderate diversity of Cisco routing and switching hardware in the network. This document should be included, as a roadmap, as part of an overall hardware replacement strategy for both short term tactical and long term strategic planning.

Reminder: The most significant End of Life milestones are (in order of occurrence): End of Software Maintenance (EoSWM), End of Vulnerability Security Support (EoVSS), and Last Date of Support (LDoS). These can affect both hardware and software. Please see Table 1 for more details on the significant milestones.

An End of Life Milestones review of the USMC managed **NIPR** network chassis inventory, totaling (b) (3), (b) (4), revealed (b) (3), (b) (4) Cisco chassis that (b) (3), (b) (4) (b) (3), (b) (4) milestones. The mission focus below indicates significant increases over the next 5 years.



The following points are critical with respect to the LDoS summary table:

- **Tactical Outlook**

- Currently, (b) (3), (b) (4). No additional issues were detected during 2019. These should be (b) (3), (b) (4) during the current budget cycle.

- **Strategic Outlook**

- A review of the timeline from (b) (3), (b) (4) indicates a significant increase in (b) (3), (b) (4) (b) (3), (b) (4). This includes (b) (3), (b) (4) and a

large (b) (3), (b) (4). The USMC IT staff is already working (b) (3), (b) (4) (b) (3), (b) (4)

- (b) (3), (b) (4) products will result in improved network performance, availability, and additional advanced features with a lower cost of support. These products are the most important to address, (b) (3), (b) (4) is the last step in Cisco's EoX timeline.
- USMC should begin budgetary planning for hardware replacements during (b) (3), (b) (4) (b) (3), (b) (4)

An (b) (3), (b) (4) review of the USMC managed **NIPR** network module inventory, which includes (b) (3), (b) (4) identified modules, (b) (3), (b) (4) modules that currently (or will (b) (3), (b) (4) (b) (3), (b) (4) mission focus below indicates significant increases over the next 5 years.

(b) (3), (b) (4)

The following points are critical with respect to the (b) (3), (b) (4)

- **Tactical Outlook**

- Currently, there (b) (3), (b) (4) (b) (3), (b) (4) the number of LDoS modules will increase by (b) (3), (b) (4) (b) (3), (b) (4) modules. Those should be targeted for replacement during the next budget cycle.

- **Strategic Outlook**

- A review of the timeline from (b) (3), (b) (4) indicates a (b) (3), (b) (4) (b) (3), (b) (4).
- (b) (3), (b) (4) with newer products will result in improved network performance, availability, and additional advanced features with a lower cost of support. These products are the most important to address, as the (b) (3), (b) (4) is the last step in Cisco's (b) (3), (b) (4).
- USMC should begin budgetary planning for hardware replacements during the (b) (3), (b) (4) (b) (3), (b) (4) budget periods.

Caveat: Transceiver modules are considered “low cost consumables” and typically discarded in the event they fail. A total of (b) (3), (b) (4) (b) (3), (b) (4) exist in the network. (b) (3), (b) (4) module count (b) (3), (b) (4) should be monitored separately from modules that would

otherwise be replaced through the RMA process. Regardless, the USMC team should begin budgetary planning for hardware replacements during the (b) (3), (b) (4) with a focus (b) (3), (b) (4) network devices.

Note: Some modules will be replaced when the parent chassis is replaced. This should be considered during budgetary planning.

This also provides the USMC team with an opportunity to further reduce hardware diversity and standardize the chassis types deployed within the USMC network. Less diversity equates to reducing the global network total cost of ownership (TCO). This strategy will require advance planning based on the future missions that USMC could be tasked to support.

Software Resiliency – Address software milestones and Software Security Vulnerabilities

At the time of the network snapshot, the MITC-West team maintained (b) (3), (b) (4) diversity with (b) (3), (b) (4) software trains deployed on the **NIPR** network. A review of the global deployment of software trains demonstrated a (b) (3), (b) (4) with like platforms running the range of (b) (3), (b) (4) release trains. The USMC team have (b) (3), (b) (4) that need to be addressed. (b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

- **Tactical Outlook**

- Currently, a total of (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)
- (b) (3), (b) (4)

- **Strategic Outlook**

- Once all the routers and switches (b) (3), (b) (4) Ongoing proactive monitoring for future (b) (3), (b) (4) (b) (3), (b) (4) incorporated into a Software Lifecycle Strategy.

Regardless of the software deployed, it is recommended that Extended Maintenance Release (EMR) trains, provided in this report, be utilized to get the maximum longevity, usually 2-3 years, from the software. EoSWM and EoVSS milestones should be considered a key performance indicator (KPI) that trigger the beginning of the planning process to upgrade the IOS on any given network device. Several IOS trains have published software advisories, indicating the presence (b) (3), (b) (4). They should be upgraded to the latest maintenance rebuild with in the current software train, if available, to take advantage of the software (b) (3), (b) (4).

This report contains baseline software train recommendations based upon the Army Enterprise Software Strategy (Army JELA Mission 51). Common Cisco hardware is found in most DOD networks, including all the MILDEPs. Organizations are strongly encouraged to consider the software releases identified by this mission as they have been pre-scrubbed with a focus on operational mission requirements.

With regard to Software Security Advisories (DoD Information Assurance Vulnerability Alert (IAVA)), this analysis revealed (b) (3), (b) (4). All software advisories should be validated with Cisco. This report includes the latest Product Security Incident Response Team (PSIRT) security vulnerability notifications as of March 2018. An effort to review the network risks and remediate those vulnerabilities found to pose significant threats to USMC should be initiated immediately.

Security Technical Implementation Guidelines (STIGs)

STIG-ID “V-3160 NET0700” states “The network element must be running a current and supported operating system with all IAVMs addressed.” Network devices that are not running the latest tested and approved versions of software are vulnerable to network attacks. Running the most current, approved version of system and device software helps the site maintain a stable base of security fixes and patches, as well as enhancements to IP security. Viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations could render a system vulnerable, allowing unauthorized access to DOD assets.

https://www.stigviewer.com/stig/layer_2_switch_-_cisco/2015-09-21/finding/V-3160

3. Technical Summary

The Technical Summary section identifies gaps between USMC resiliency and related operational practices and Cisco identified leading practices for resilient highly available network environments. The section includes an overview of the assessment findings and a summary table (Table 1) showing the gaps identified and recommendations for each practice. More detail regarding each area can be found in the assessment detail section of the report.

3.1. Introductory Comments

The Cisco Advanced Services team wishes to thank all of the participants involved in the data gathering phases of the ALA. The MITC-West team individuals were professional, knowledgeable and open about the USMC processes for asset management. They provided us with insight into the network and organization that would have been impossible to attain otherwise.





The Cisco Advanced Services team and the Cisco Account team are planning to meet with USMC management to further discuss our recommendations for addressing the issues highlighted in this assessment.

3.2. Assessment Process


The assessment process is a phased analysis approach that helps to ensure a thorough investigation into USMC asset supportability. The assessment is delivered by the Cisco Advanced Delivery Network Services (ADN) and Joint Enterprise Level Agreement (JELA) Teams with input from key Cisco Advanced Services technology experts. The delivery team also utilizes network tools to analyze hardware diversity and software diversity.

The Summary Findings section provides a summary and overview of the identified gaps in relation to Cisco's identified leading practices. Each of the functional areas is evaluated against best-practice criteria within the identified area. Table 1 lists each of the seven functional areas along with their leading practice conformance rating and corresponding recommendations based on the following color scheme:

Table 1: Maturity Level Color Coding

	Green is assigned when conformance to the best-practice exists
	Yellow is assigned when partial conformance to the best-practice exists
	Red is assigned when little or no conformance to the best-practice exists
	Blue is assigned when the particular area was not evaluated

(b) (3), (b) (4)



4. Assessment Detail

This section of the assessment contains detailed findings, recommendations and additional detail on Cisco identified leading practices for the ALA. You can use this section as a reference to understand detailed findings and recommendations for each of the identified assessment areas.

4.1. Hardware Resiliency

Hardware Resiliency is an analysis of the Cisco chassis and modules used to design the network.

- General Hardware Information – refers to the network chassis and modules used in the network.
- Modularity – refers to using the same device for the same network function throughout the network
- Scalability – refers to the age of the equipment, ability to support newer high availability features and the ability to support performance goals
- Hardware Replacement and Refresh Strategy – identifies availability issues within specific component groups

4.1.1. Recommendations

The Cisco team has the following recommendations in the hardware resiliency section:

- **(b) (3), (b) (4) network hardware elements that have (b) (3), (b) (4) milestones to ensure hardware supportability. (b) (3), (b) (4)**
(b) (3), (b) (4).
This includes **(b) (3), (b) (4)**
(b) (3), (b) (4) announcements for guidance on the Cisco recommended standard replacements. If additional features are to be considered, consult your Cisco Systems Engineer (SE).
- **Tactical – Begin the planning process to replace hardware that will reach its (b) (3), (b) (4) milestone (b) (3), (b) (4) calendar years. (b) (3), (b) (4)** a trigger milestone since Cisco **(b) (3), (b) (4)** for the platforms affected. **(b) (3), (b) (4)** milestone soon. Future replacements should be identified and budgetary planning initiated. Evaluate **(b) (3), (b) (4)** **(b) (3), (b) (4)** recommended replacements.
- **Strategic – Identify, document, and implement formal hardware refresh triggers using this report as a baseline for current or future hardware refresh processes.** Using formal triggers (**(b) (3), (b) (4)**) will allow the organization to track milestones and make consistent budgeting decisions from a proactive posture instead of reacting to outages and recurring incidents. A good place to start would be to **(b) (3), (b) (4)** milestones published by Cisco and provided to USMC.

- **Strategic – Incorporate formal hardware refresh triggers into the existing hardware refresh strategy** to guarantee hardware supportability. Utilize Cisco Notification Services to gain receive alerts regarding hardware lifecycle announcements. A documented refresh strategy, with reportable triggers, enables the organization to accurately create quarterly and annual budgets that can be used to justify hardware replacement. As a result, support should always be maintained on any hardware installed in the network. Additionally, network maintenance costs are reduced by eliminating the possibility for outages due to aging network hardware. Hardware currency also plays a significant role in software supportability in that newer hardware is more likely to support the latest software releases and features.
- **Strategic – Identify and document all warehoused hardware inventory.** Assets that are stored//warehoused must be inventoried on a regular basis to maintain End of Life status awareness. Failure to maintain these assets could negatively impact the USMC mission. Each asset should be powered ON to verify proper operation and the End of Life status of the IOS running on the asset verified and/or upgraded to maintain readiness.
- **Strategic – Identify and document all suspicious inventory that appears to be either grey market or counterfeit hardware.** The USMC network could possibly have suspicious network hardware in its inventory. Counterfeit and unauthorized secondary market (commonly referred to as grey market) products and components introduce risks with regard to the quality, reliability, and safety of network devices and network performance, whether through substandard components, inadequate testing and manufacturing, or the use of pirated, unauthorized, and unlicensed software. The authenticity of any suspect hardware should be reported and verified through Cisco before use.

4.1.2. General Hardware Information Observations


The USMC network consists of a variety of chassis and modules. Device show commands were collected by Cisco and USMC personnel from (842) network devices, which include a number of switch stacks. The following charts and tables provide an overview of the routers, switches, modules, security appliances, and firewalls analyzed and collected during this assessment. Included in the following charts and tables are Alerts for chassis and modules that are currently impacted by End of Life (EoL) announcements.

Hardware Migration Recommendations

This report includes an EoX spreadsheet that contains migration product information for hardware that has reached or will reach End of Life status.

SCE Comments: It should be noted that the EoX report spreadsheet provides default migration hardware information which is typically NOT provided with this report. Customers are **STRONGLY** encouraged to engage their Cisco Account Team - Systems Engineer (SE) for migration information based on potential future network designs and applications requirements. If this is not required, see the file “DON95_Camp Pendleton_NIPR_ALA.xlsx” included with this report.


(b) (3), (b) (4)



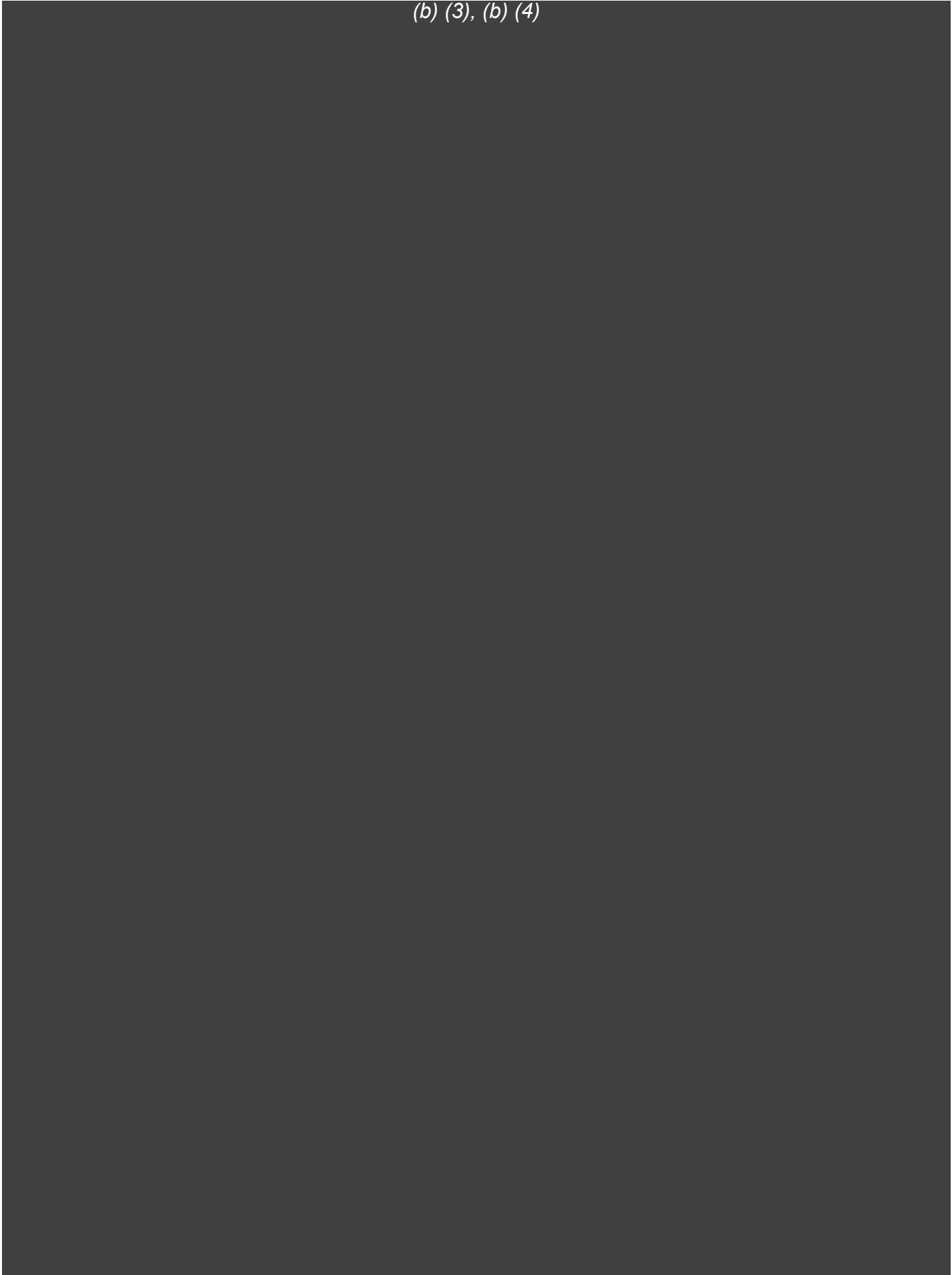
(b) (3), (b) (4)




(b) (3), (b) (4)



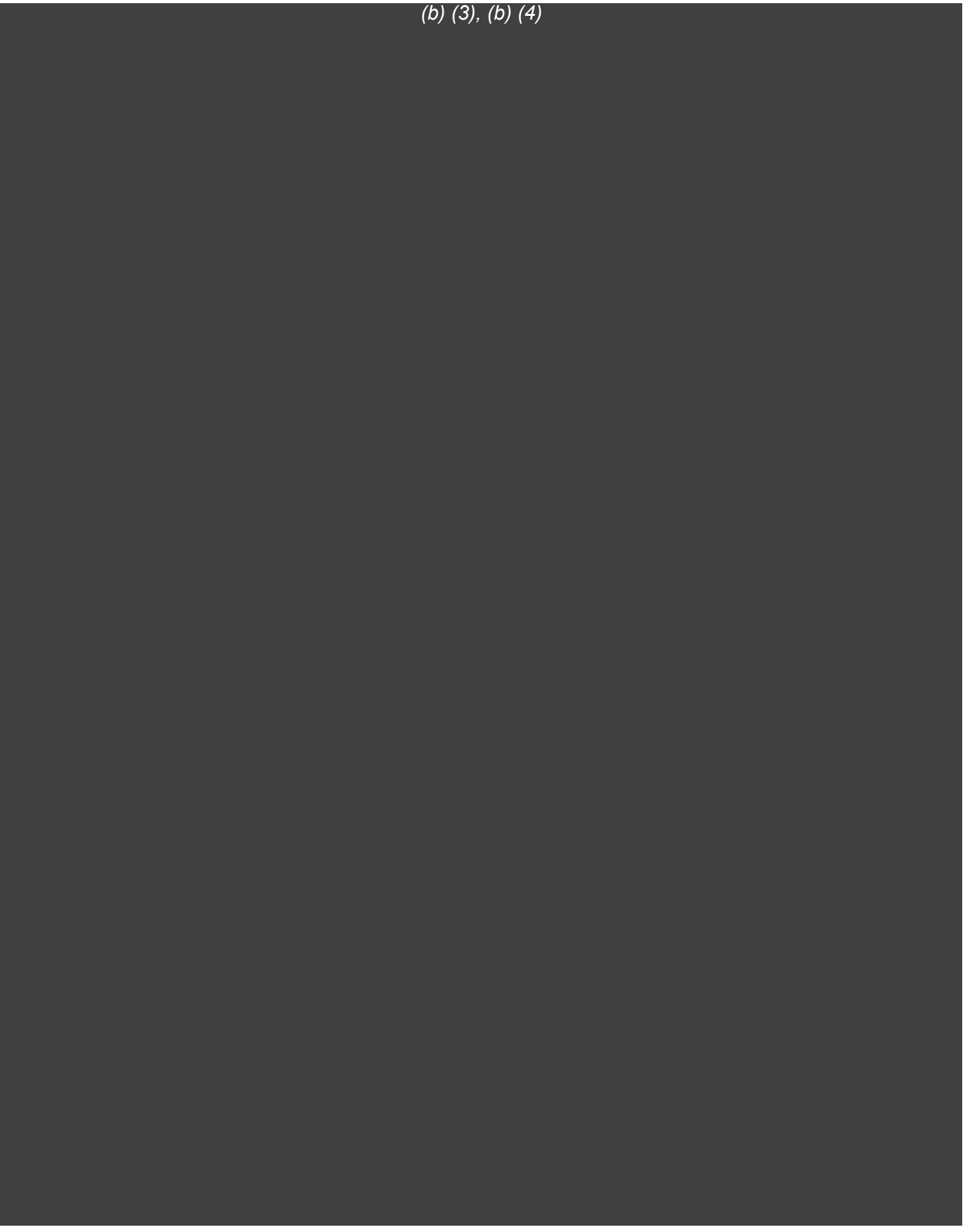
(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)



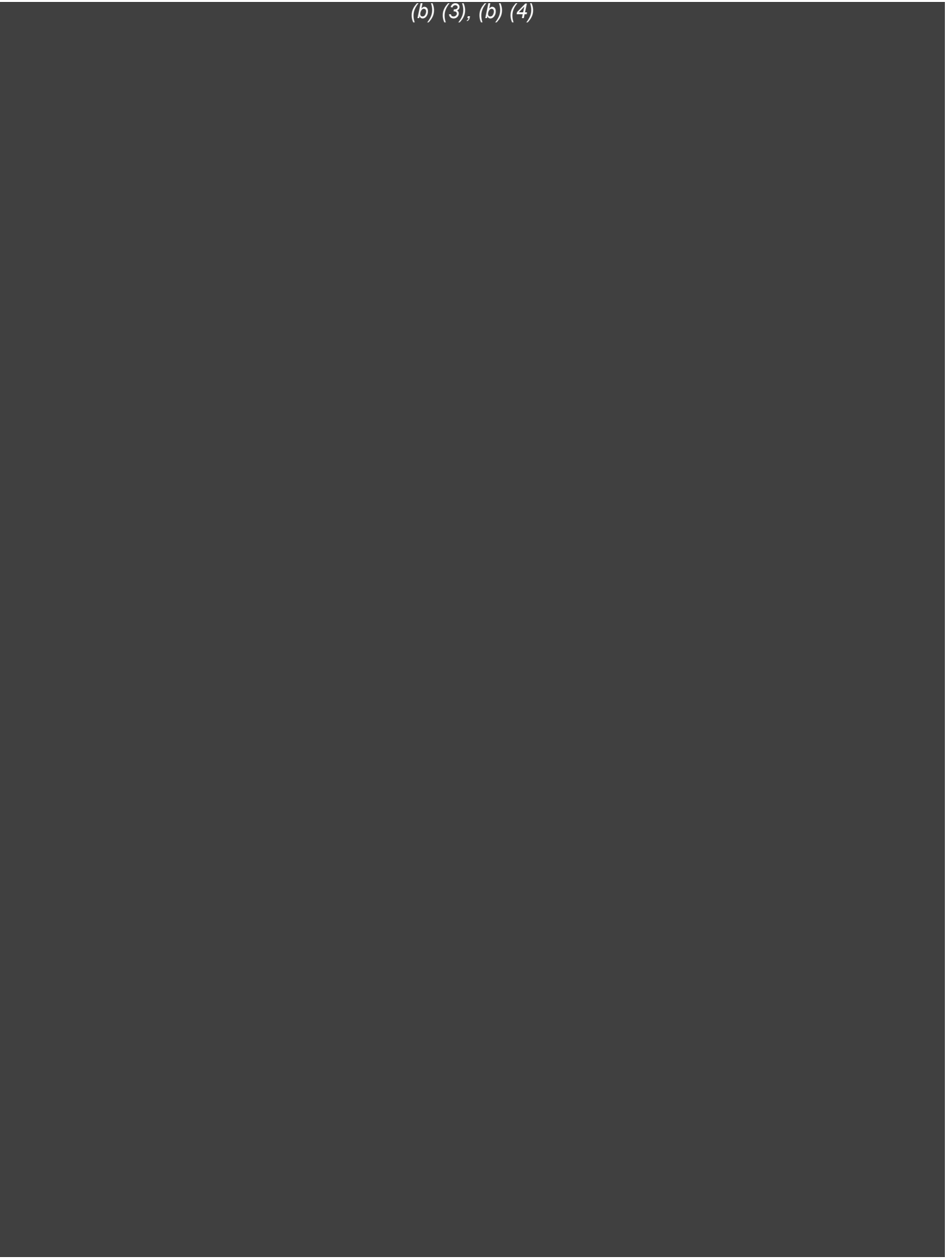
(b) (3), (b) (4)



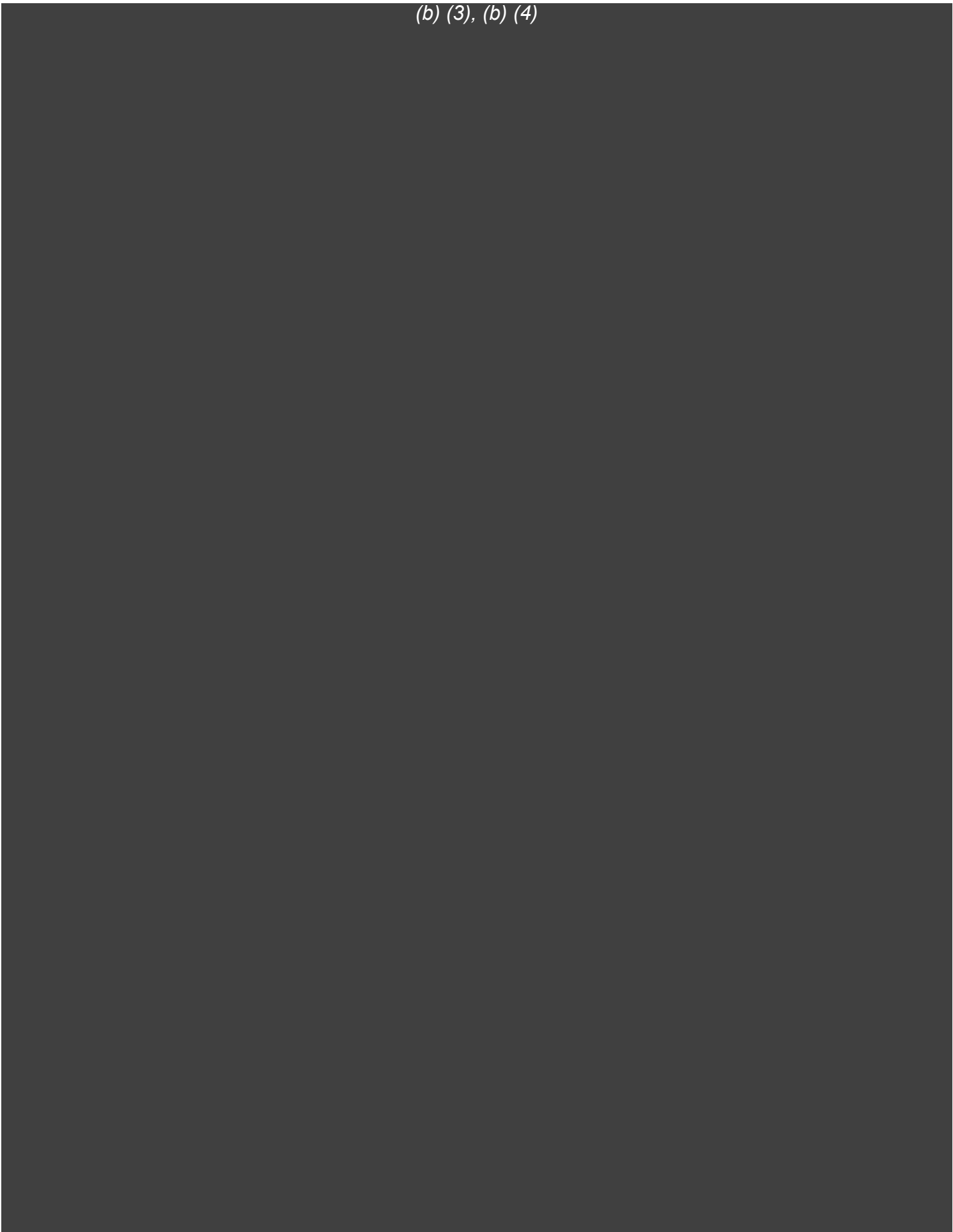
(b) (3), (b) (4)



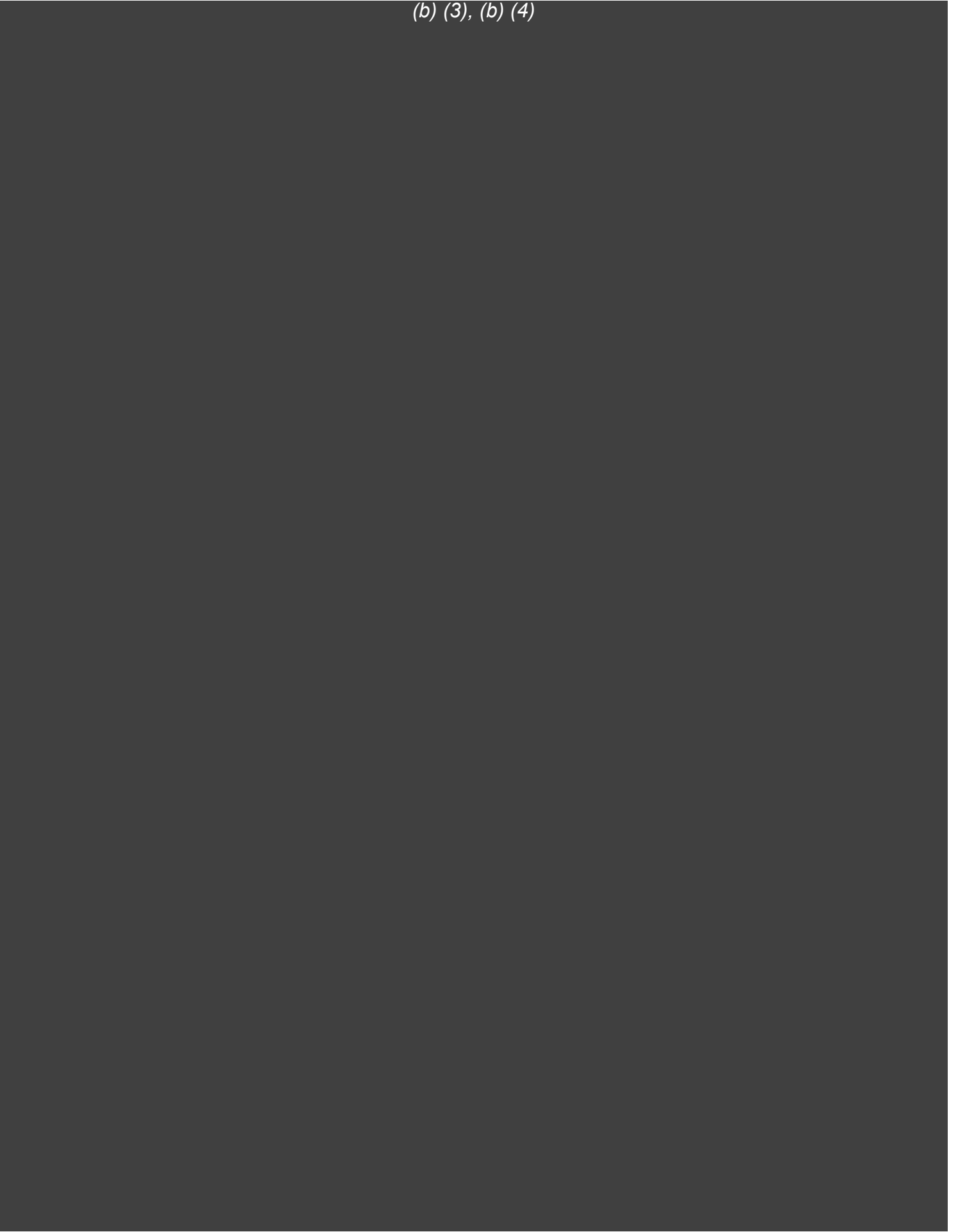
(b) (3), (b) (4)



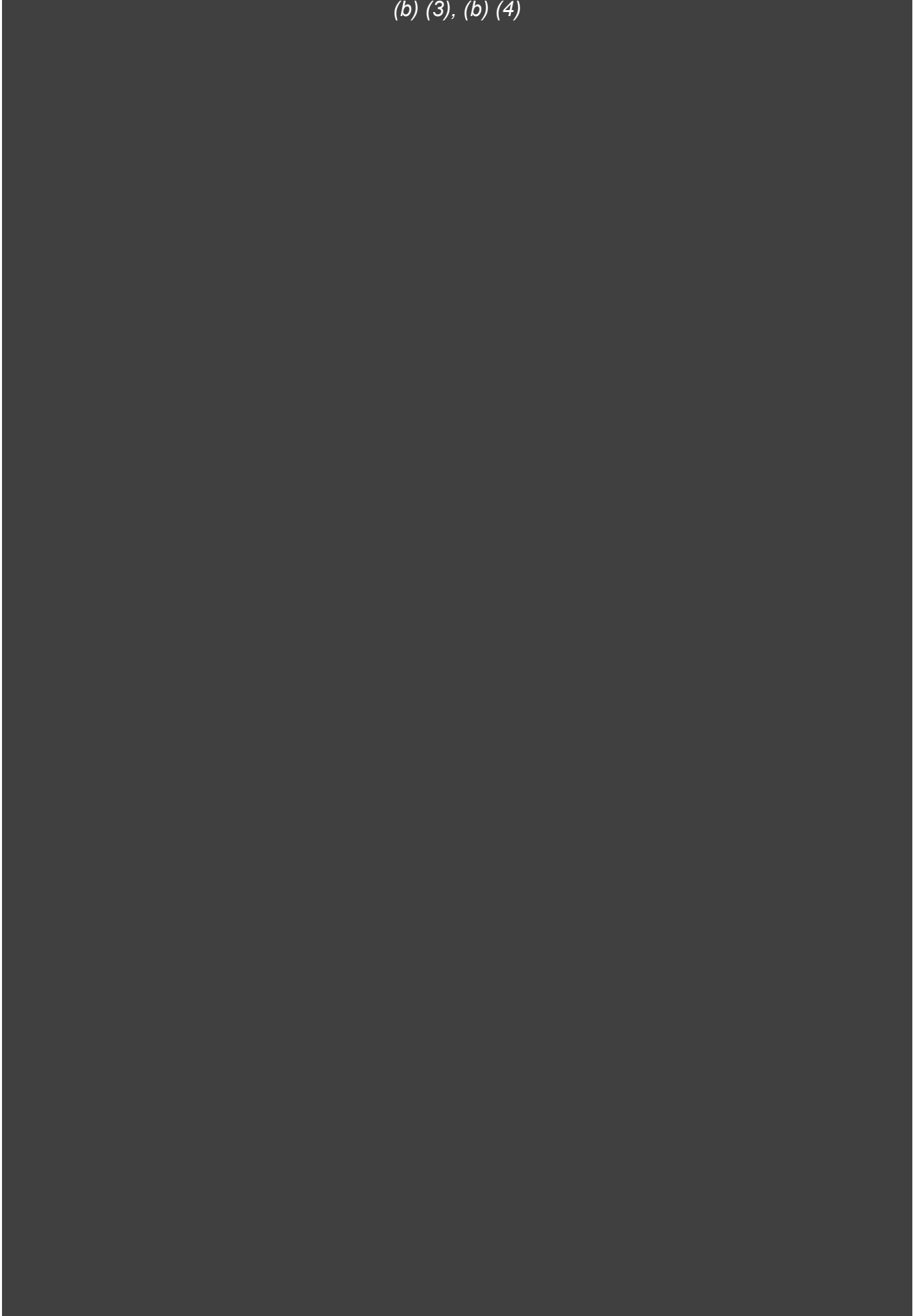
(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)



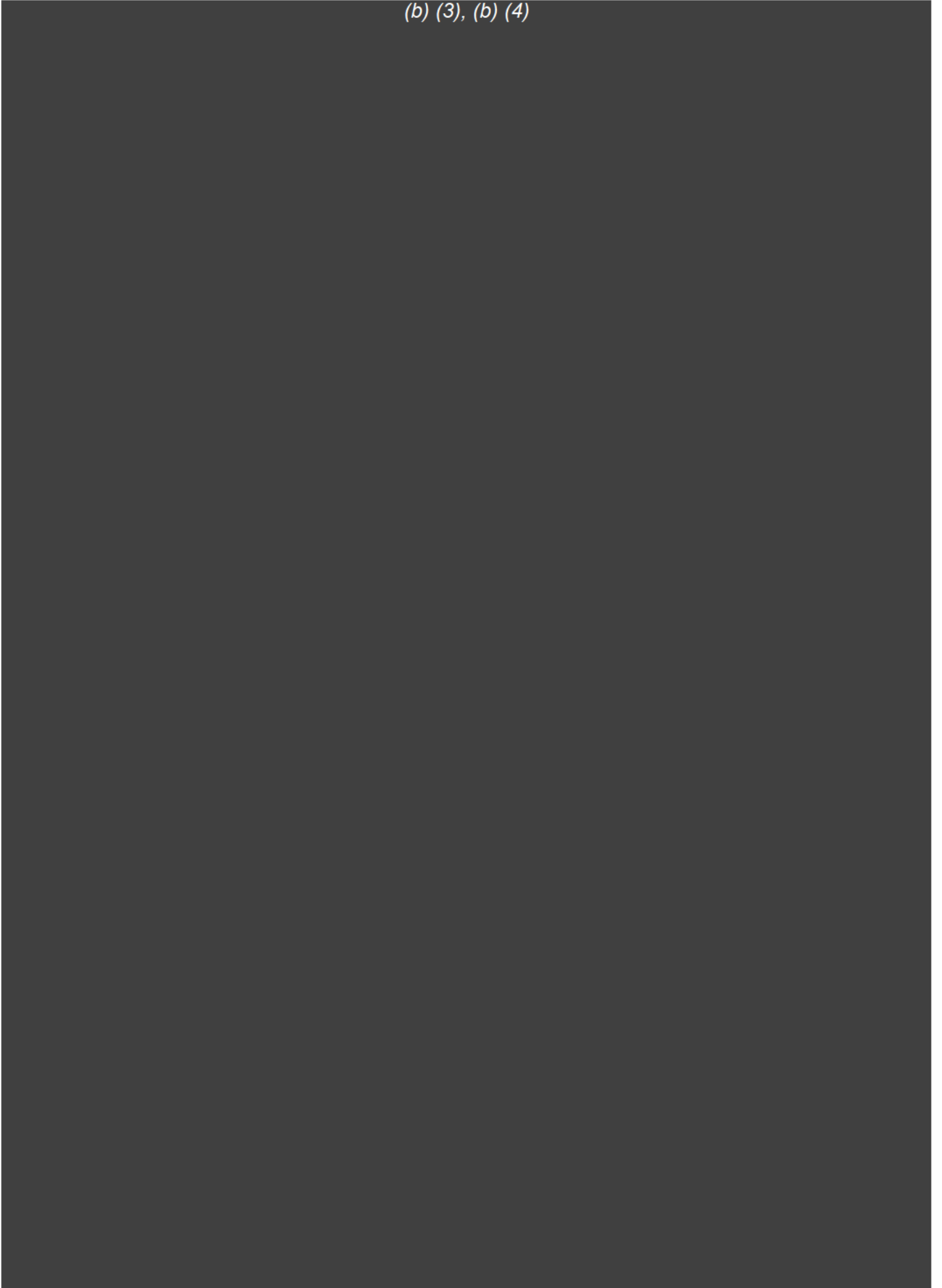
(b) (3), (b) (4)



(b) (3), (b) (4)




(b) (3), (b) (4)



4.2. Software Resiliency

Software Resiliency focuses on currently deployed device operating software as well as processes used to plan, design, implement, and operate Cisco software in a mid- to large-scale


(b) (3), (b) (4)



4.2.1. Recommendations:

The Cisco team has the following recommendations in the Software Resiliency analysis section:

(b) (3), (b) (4)



(b) (3), (b) (4)

4.2.2. Software Release Management Observations

Onsite interviews with USMC team leads indicated that (b) (3), (b) (4), the USMC team does an excellent job of maintaining consistency in the various (b) (3), (b) (4) in the network. It is obvious from the network data collected that (b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

4.2.3. Software Security Advisories Observations

The Cisco PSIRT releases bundled Software Security Advisories notifications (b) (3), (b) (4), (b) (3), (b) (4), (b) (3), (b) (4)

Cisco routinely releases updated software fixes and workarounds to address potential security vulnerabilities. Leading practice is to evaluate published vulnerabilities and remediate those that put the USMC network at risk. This includes upgrading software with software fixes included.

Interviews found that (b) (3), (b) (4), (b) (3), (b) (4), (b) (3), (b) (4)

(b) (3), (b) (4) The following tools can be used when checking for software security advisories. (b) (3), (b) (4)

(b) (3), (b) (4)

Leading practice is to evaluate published vulnerabilities and remediate those that potentially put (b) (3), (b) (4) at risk. This includes (b) (3), (b) (4) upgrading software with software fixes included. The (b) (3), (b) (4)

(b) (3), (b) (4)

In addition, Cisco routinely releases updated software fixes and workarounds to address potential security vulnerabilities. These advisories are (b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

This ALA report provides general software guidance based on no less than three (3) sources. Those resource are:

(b) (3), (b) (4)

Baseline software recommendations are based on (b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

STIG Requirements

STIG-ID “V-3160 NET0700” states “The network element must be running a current and supported operating system with all IAVMs addressed.” Network devices that are not running the latest tested and approved versions of software are vulnerable to network attacks. Running the most current, approved version of system and device software helps the site maintain a stable base of security fixes and patches, as well as enhancements to IP security. Viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations could render a system vulnerable, allowing unauthorized access to DOD assets.

(b) (3), (b) (4)

4.2.4. Software Lifecycle Management Observations

Network data indicates that a number of (b) (3), (b) (4)

(b) (3), (b) (4)

(b) (3), (b) (4)

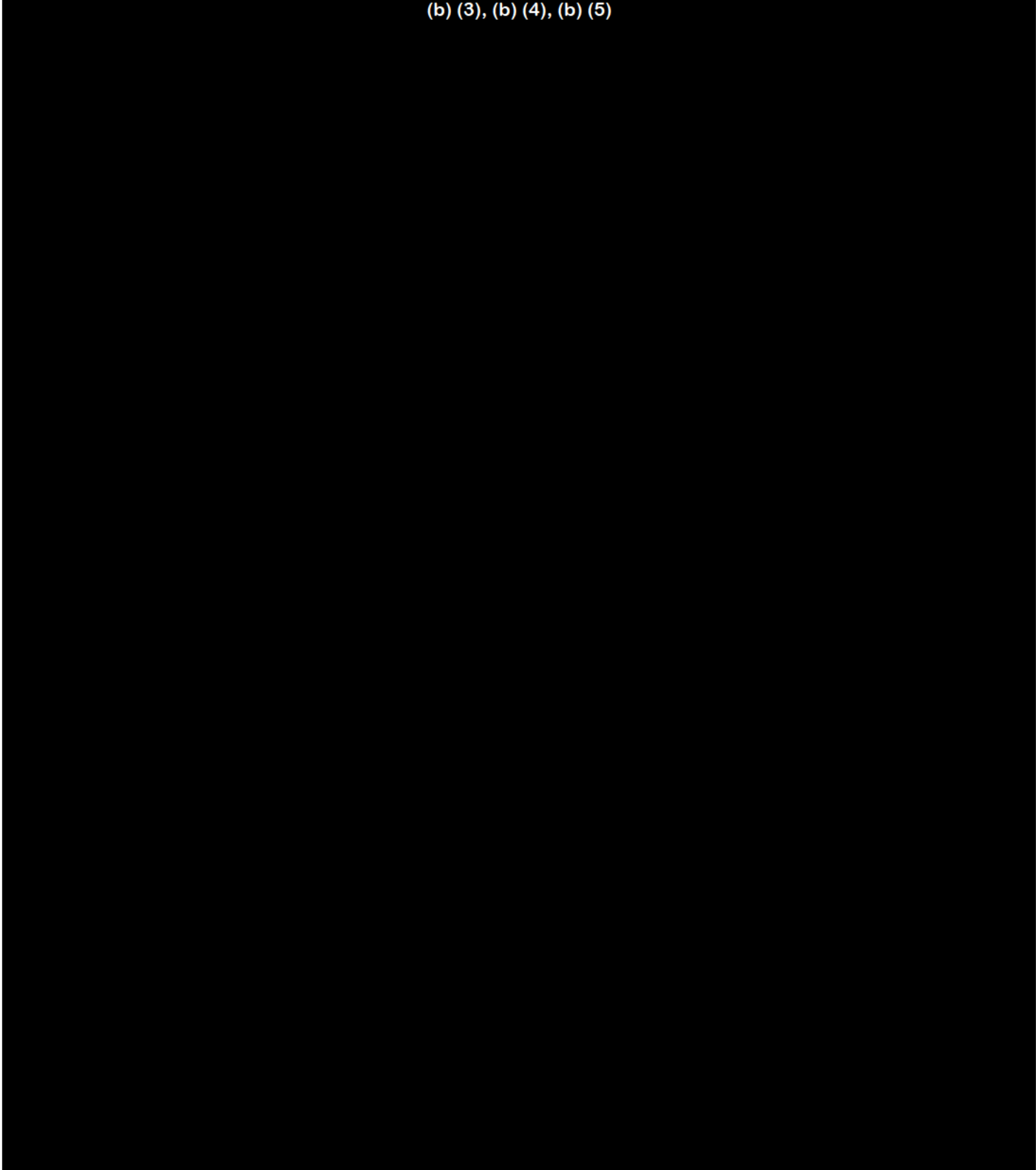
4.2.5. Software Analysis

(b) (3), (b) (4)


(b) (3), (b) (4)

to indicate specific milestones.


(b) (3), (b) (4), (b) (5)




(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)



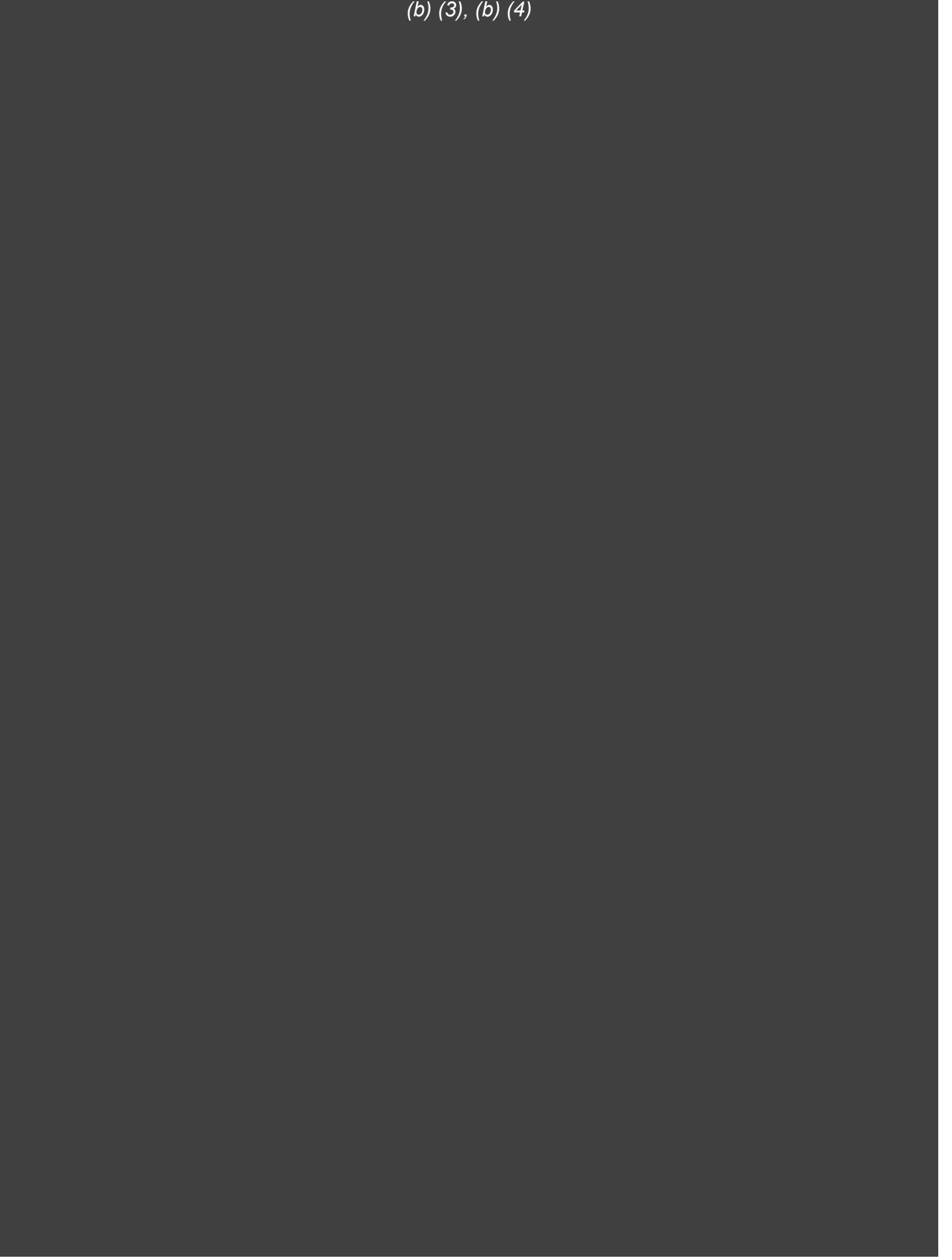
(b) (3), (b) (4)




(b) (3), (b) (4)



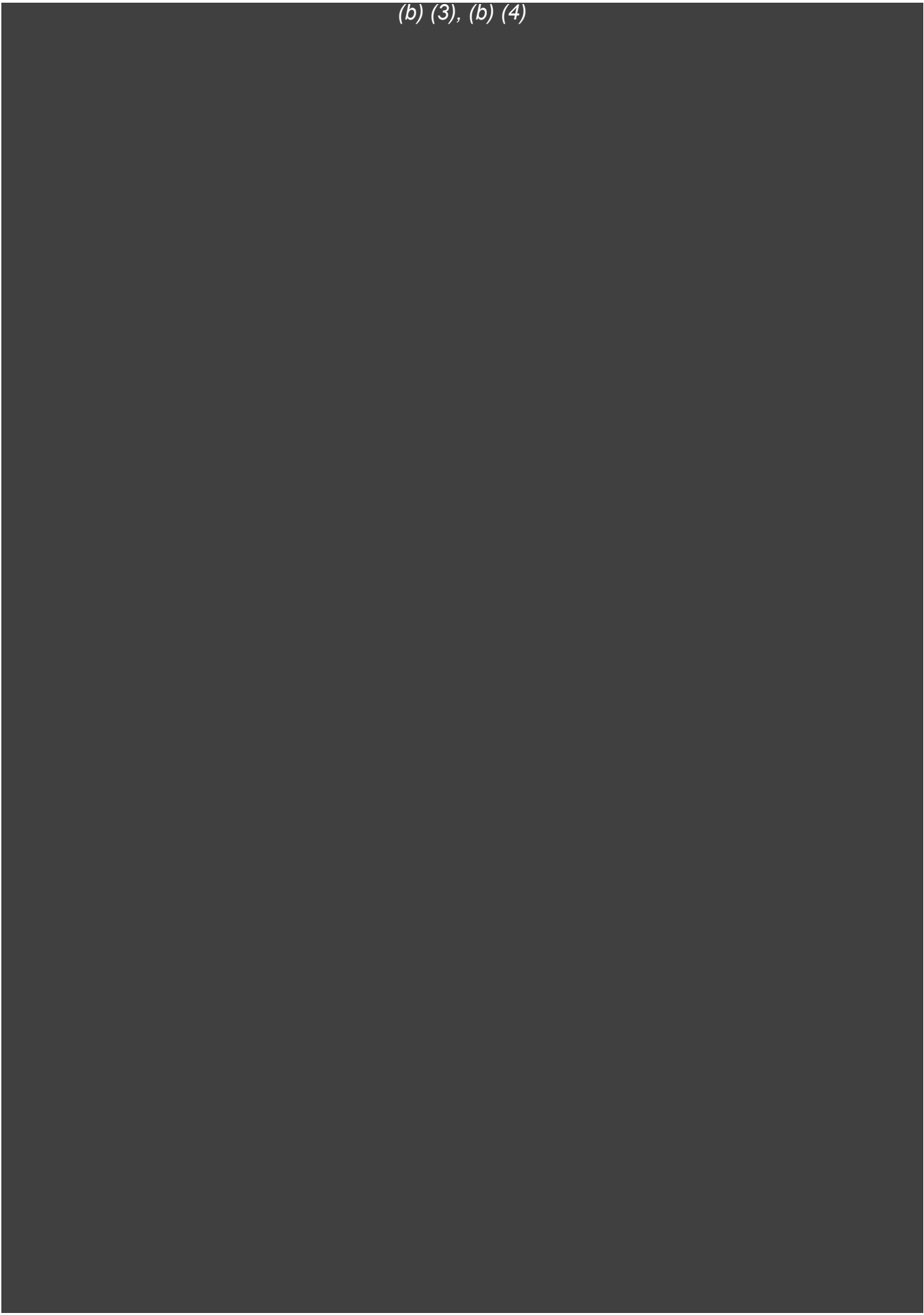
(b) (3), (b) (4)




(b) (3), (b) (4)



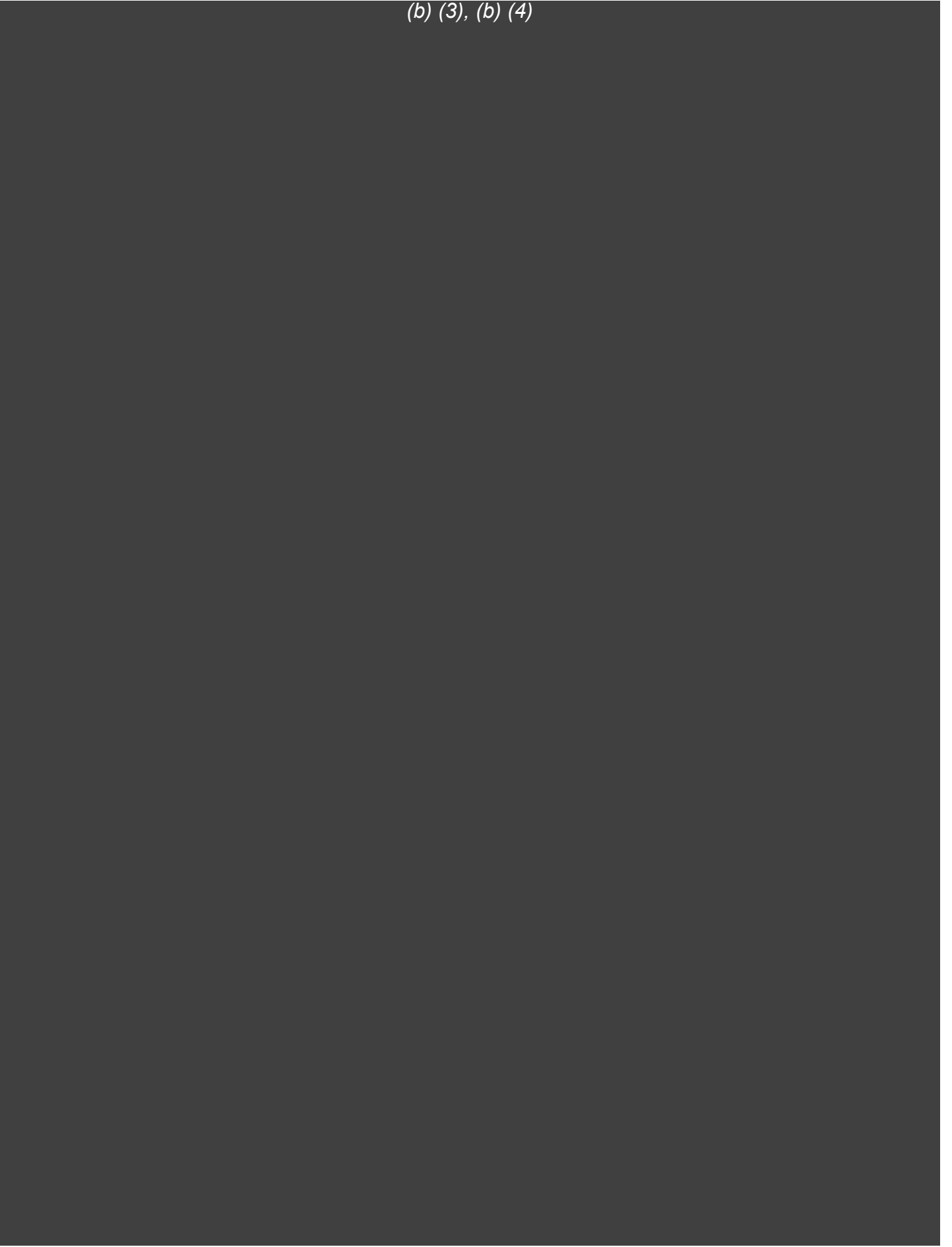
(b) (3), (b) (4)



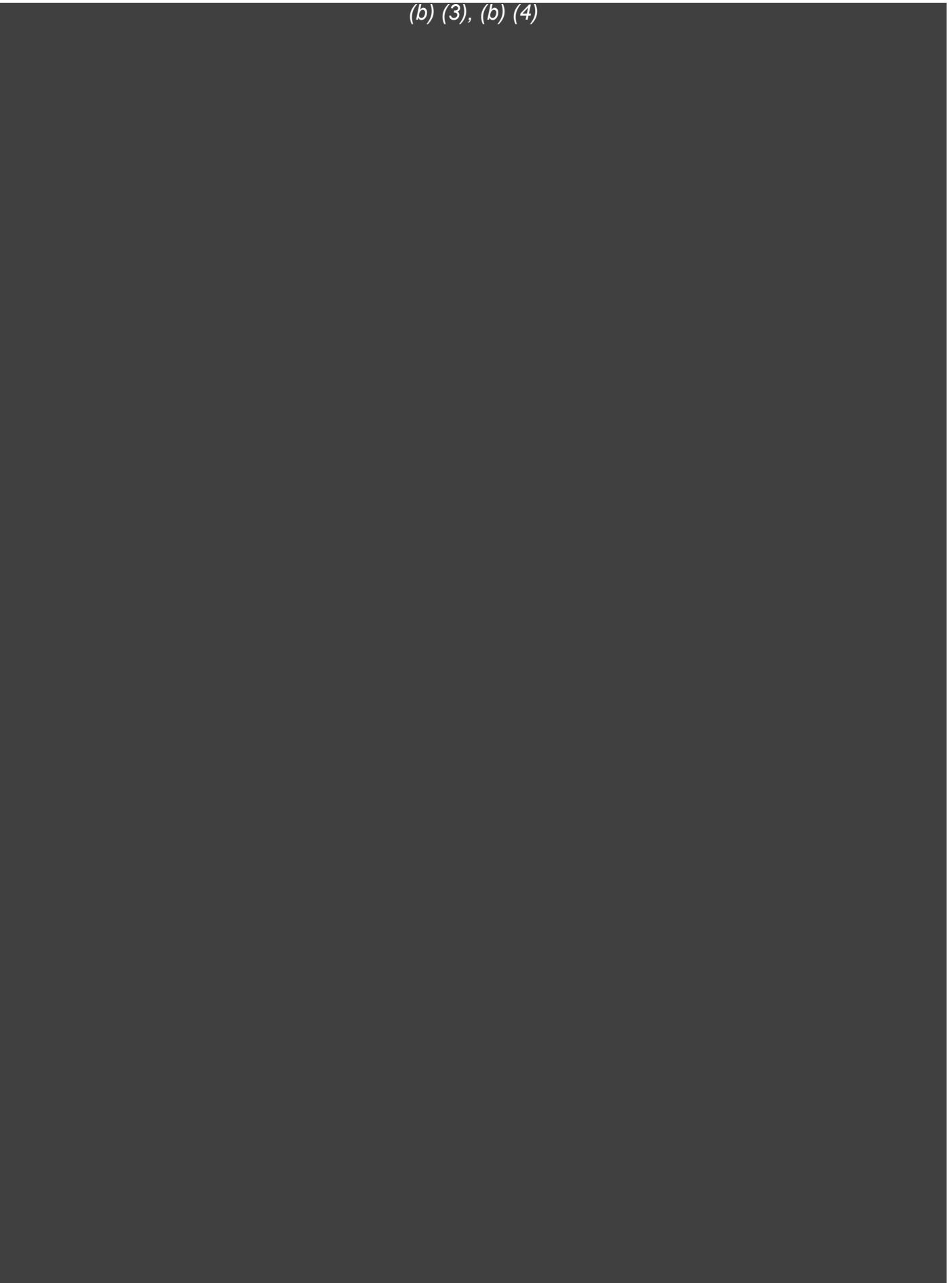
(b) (3), (b) (4)



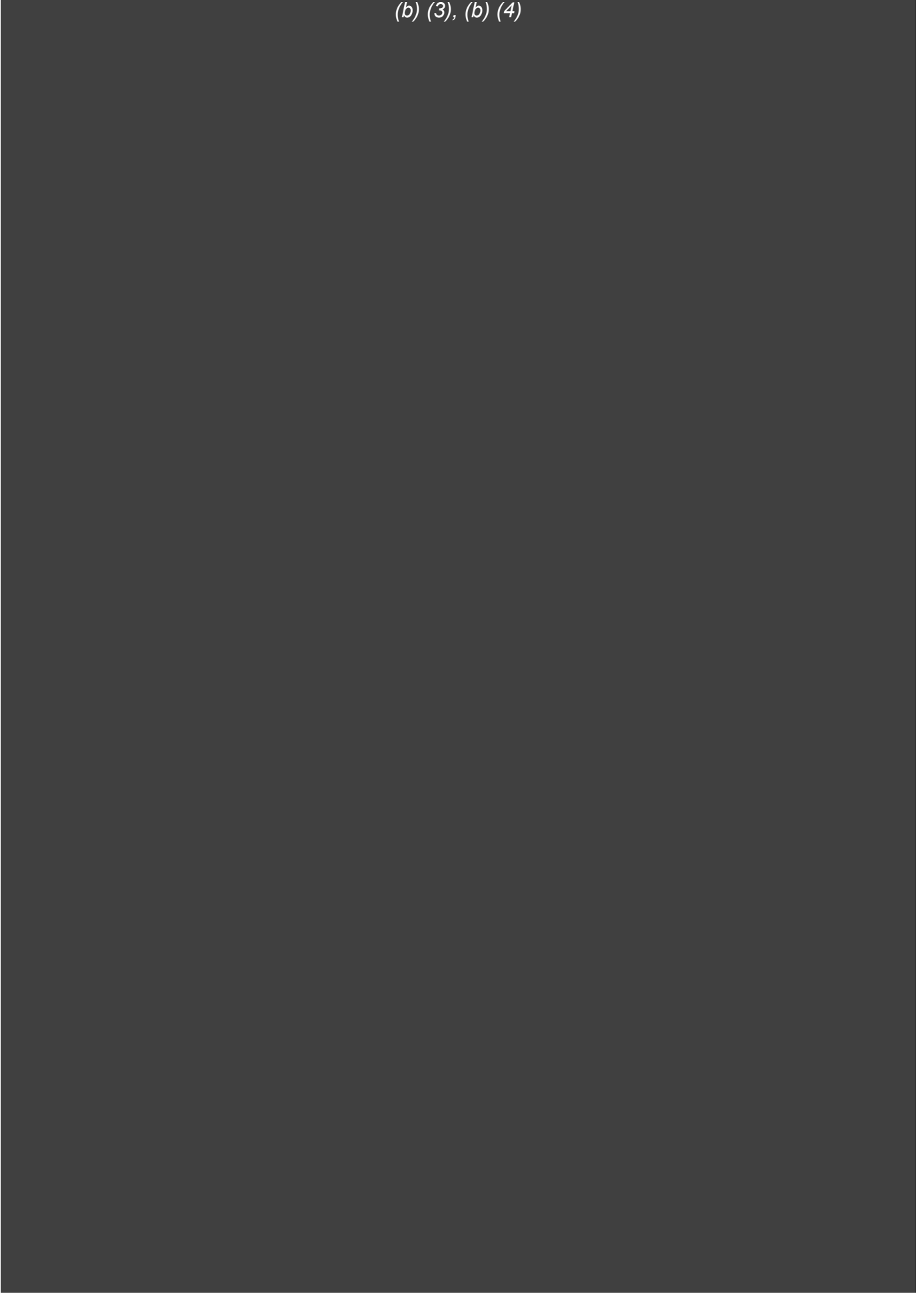
(b) (3), (b) (4)



(b) (3), (b) (4)



(b) (3), (b) (4)



5. USMC and Cisco Participants

5.1. USMC Team



USMC - ALA Point of Contact:

Name	Role / Organization
(b) (6)	

5.2. Cisco Team



Name	Role / Organization
<div data-bbox="168 527 1401 638"></div>	

Appendix A – Acronyms

Acronym	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ATA	Advanced Technology Attachment
BGP	Border Gateway Protocol
BNA	BMC Network Automation
BPDU	Bridge Protocol Data Unit
CAM	Content Addressable Memory
(b) (4)	
CNS	Classified Network Support
CoE	Center of Excellence
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DNS	Domain Name System
DTP	Dynamic Trunking Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EMR	Extended Maintenance Release
EoL	End of Life
EoRFA	End of Routine Failure Analysis
EoSale	End of Sale
EoSCR	End of Service Contract Renewal
EoSWM	End of Software Maintenance
EoVSS	End of Vulnerability/Security Support
EoX	End of X
GLBP	Gateway Load Balancing Protocol
GMRP	GARP Multicast Registration Protocol

Acronym	Definition
HA	High Availability
HSRP	Hot Standby Router Protocol
IAVA	Information Assurance Vulnerability Alerts
ICMP	Internet Control Message Protocol
IFS	IOS Files System
IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
IPS	Intrusion Prevention Systems
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology System Management
KPI	Key Performance Indicator
LDoS	Last Day of Support
MD5	Message Digest 5
MOP	Maintenance Operation Procedures
MTBF	Mean Time Between Failure
MTTR	Mean Time to Restore/Repair
NAP	Network Access Point
NARC+	Network Availability and Reliability Calculation Plus
NCM	Network Compliance Manager
NETCOM	Network Enterprise Technology Command
NIP	Network Improvement Plan
NIPRnet	Unclassified but Sensitive Internet Protocol Network
NMS	Network Management System
ALAP	Asset Lifecycle Analysis Plan
NRA	Network Resiliency Analysis
NSF	Non-Stop Forwarding
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
OOMB	Out of Band Management
OSPF	Open Shortest Path First
PAD	Packet Assembler/Disassembler
PAgP	Port Aggregation Protocol

Acronym	Definition
PCMCIA	Personal Computer Memory Card International Association
PIC	Payment Card Industry
PID	Part Identification Number
PSIRT	Product Security Incident Response Team
PSU	Power Supply Units
PVST+	Per VLAN Spanning Tree Plus
QBR	Quarterly Business Reviews
USMC	Regional Cyber Center – Western Hemisphere
RFC	Request for Change
ROMMON	ROM Monitor Mode
RP	Route Processor
RPF	Reverse Path Forwarding
RR	Route Reflector
RRC	Router Reflector Candidates
SHARC+	System Hardware Availability and Reliability Calculation Plus
SIPRNet	Secret Internet Protocol Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SPoF	Single Point of Failure
SSH	Secure Shell
SSO	Stateful Switch Over
STIG	Security Technical Implementation Guide
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCO	Total Cost of Ownership
TLA	Top Level Architecture
TLV	Type-Length-Value
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
UDLD	Unidirectional Link Detection
UDP	User Datagram Protocol

Acronym	Definition
VDC	Virtual Device Context
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VPLS	Virtual Private LAN Service
VPN	Virtual Path Number
VRF	VPN Routing and Forwarding
VTP	Virtual Trunking Protocol
WOL	Wake-on-LAN

Appendix B – LDoS Summaries by Year 2018-2023

The following charts and tables contain summaries of the

(b) (3), (b) (4)

(b) (3), (b) (4)

LDoS Chassis Summary – Now

(b) (3), (b) (4)

LDoS Chassis Summary – 2019

None

Figure 43: LDoS Chassis Summary – 2019

Device Chassis	Chassis Count	Status	Date	End of Life Notice
	0			
Totals	0			

LDoS Chassis Summary – 2020

LD

(b) (3), (b) (4)

--	--	--	--	--

Figure 44: LDoS Chassis Summary – 2020

(b) (3), (b) (4)

--	--	--	--	--

LDoS Chassis Summary – 2021

(b) (3), (b) (4)


--	--	--	--	--

Figure 45: LDoS Chassis (b) (3), (b) (4)


(b) (3), (b) (4)

--	--	--	--	--


(b) (3), (b) (4)




(b) (3), (b) (4)



(b) (3), (b) (4)



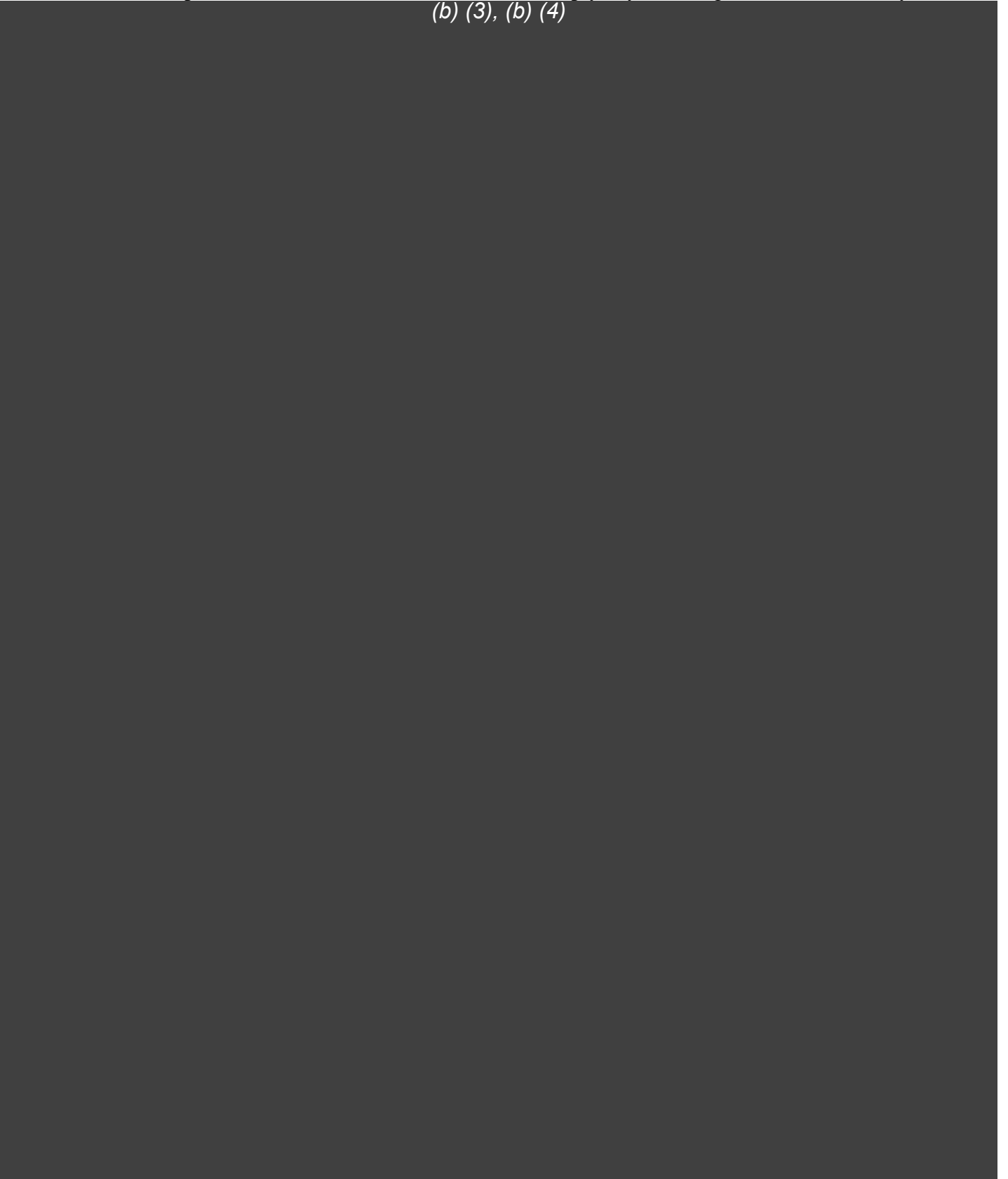
(b) (3), (b) (4)



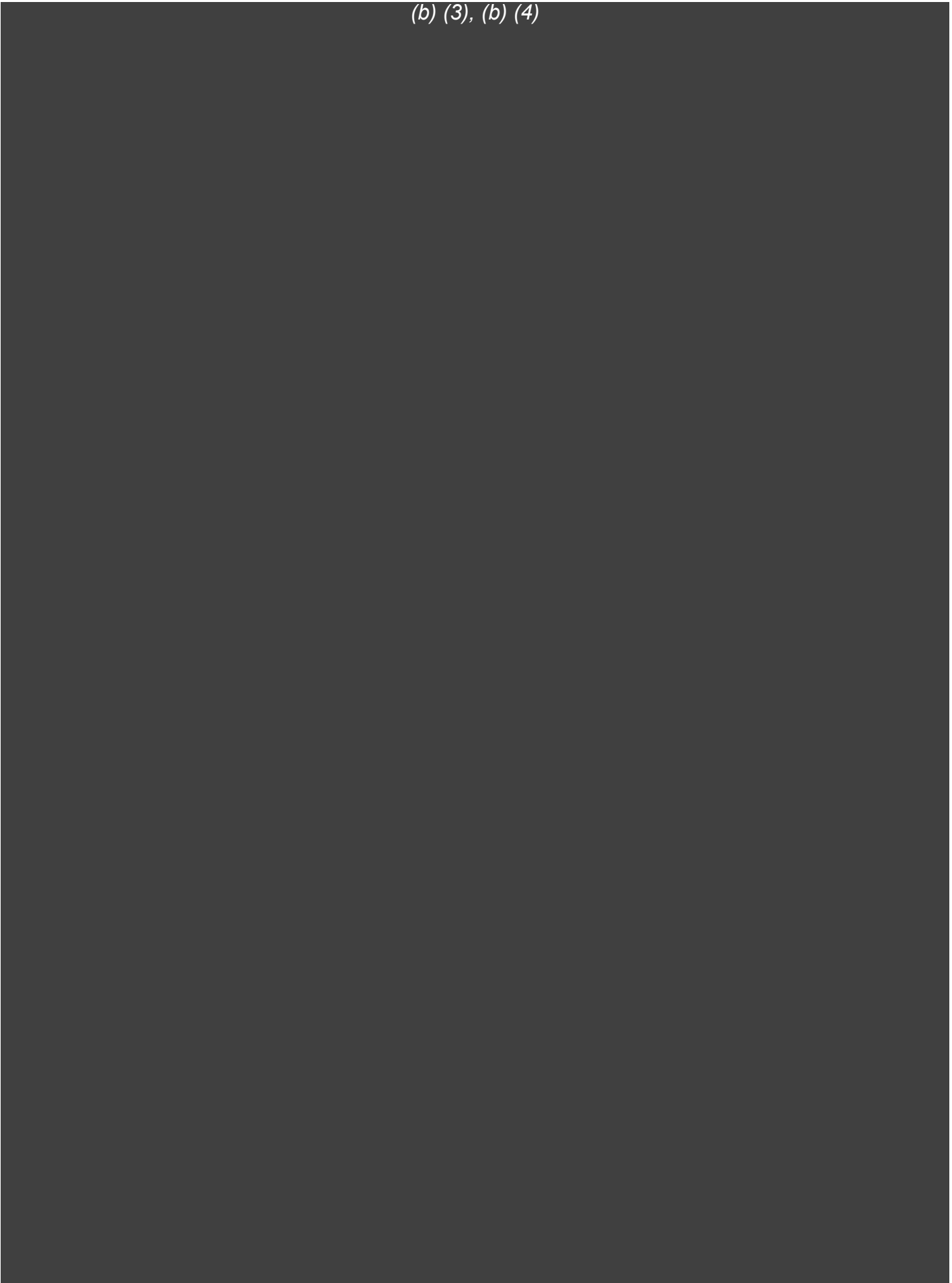
Appendix C – Cisco Security Advisories

The information provided on an 'as is' basis and does not imply any kind of guarantee or warranty.

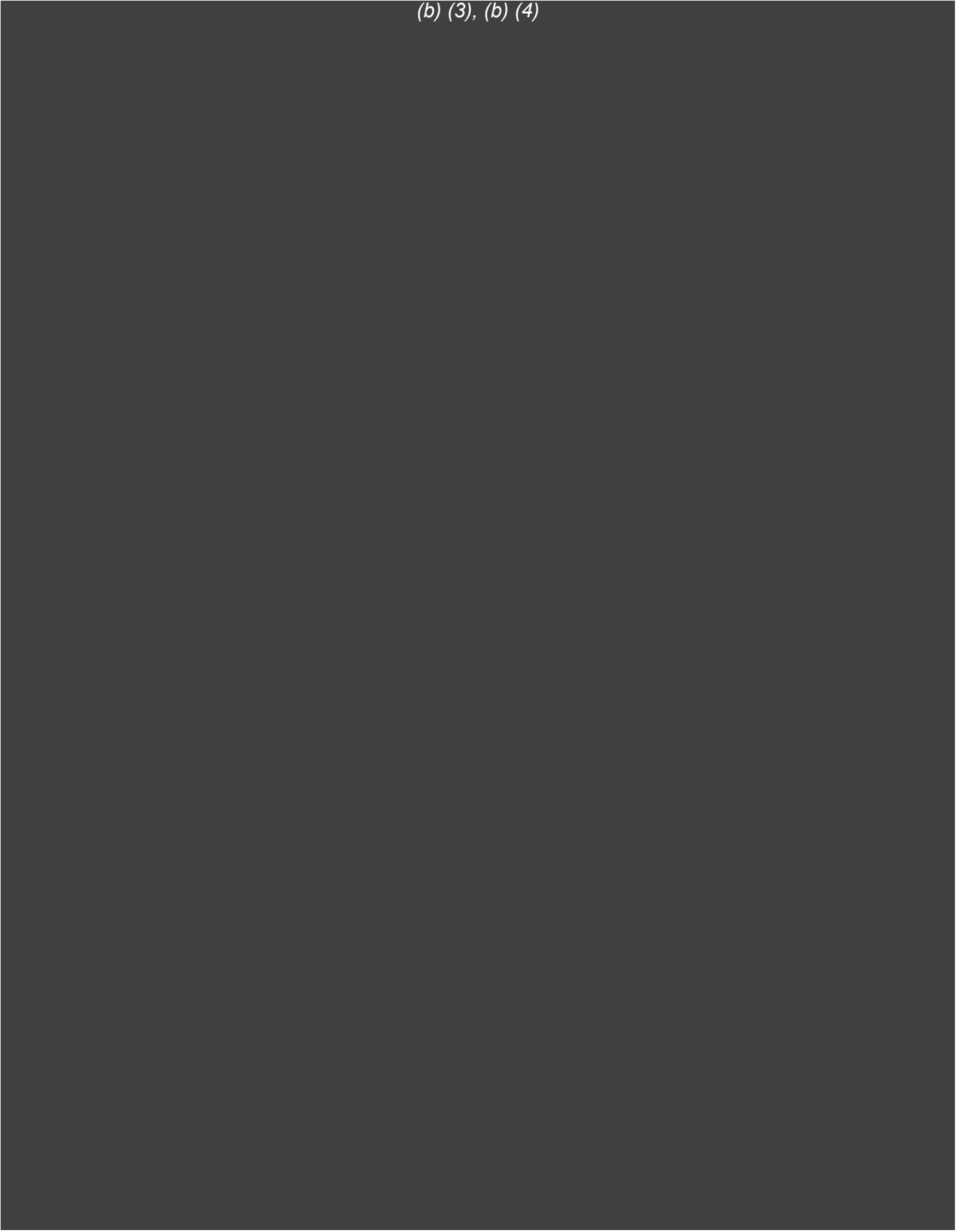
(b) (3), (b) (4)




(b) (3), (b) (4)



(b) (3), (b) (4)



(b) (3), (b) (4)




Appendix D – LDoS Now Chassis

The chassis shown in the tables that follow have surpassed their Last Date of Support (LDoS) milestones. To meet STIG requirements, the hardware//software must be supported by Cisco. While newer software release trains may still support the hardware; the hardware cannot be replaced via

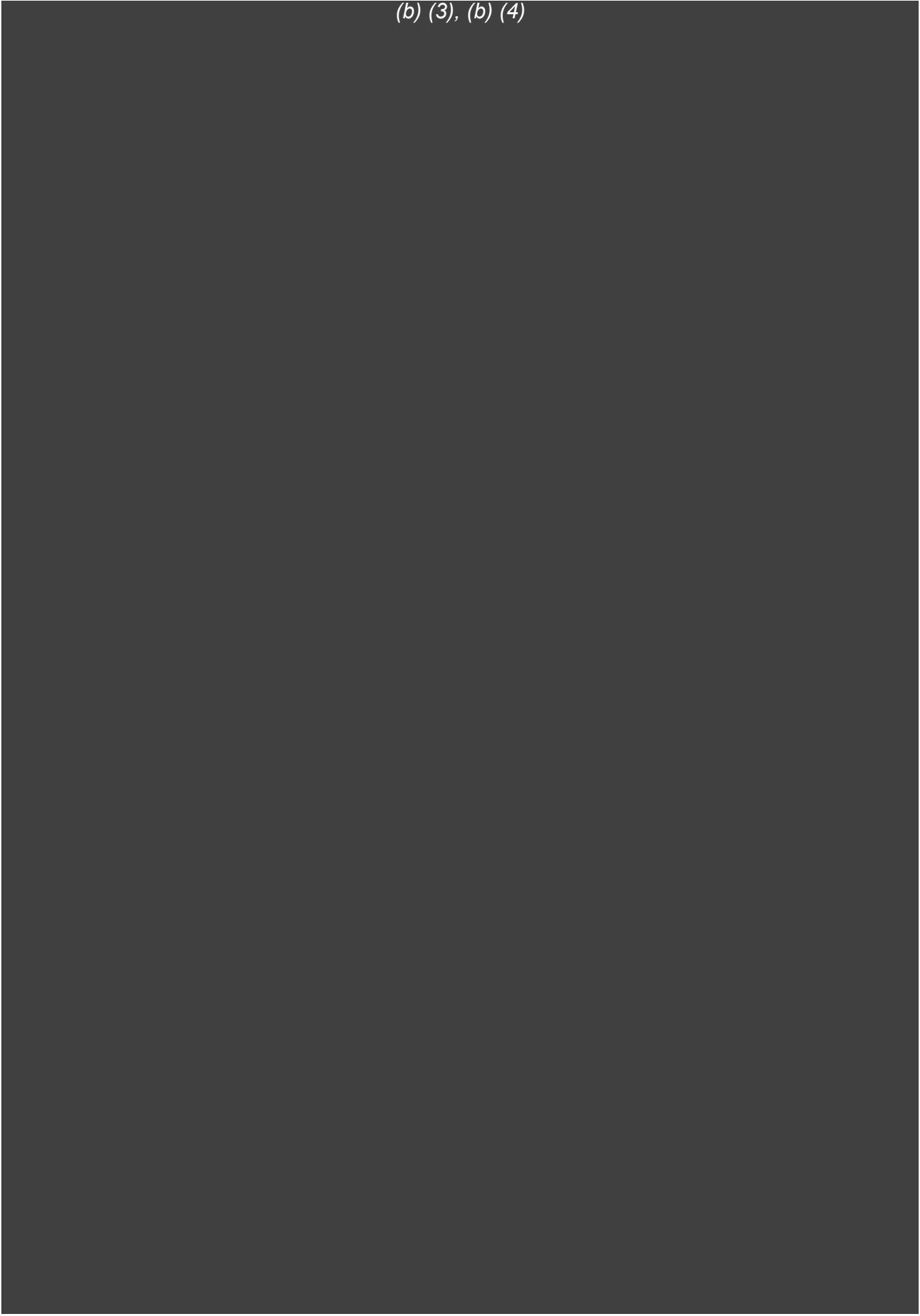
(b) (3), (b) (4)

(b) (3), (b) (4)


(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)



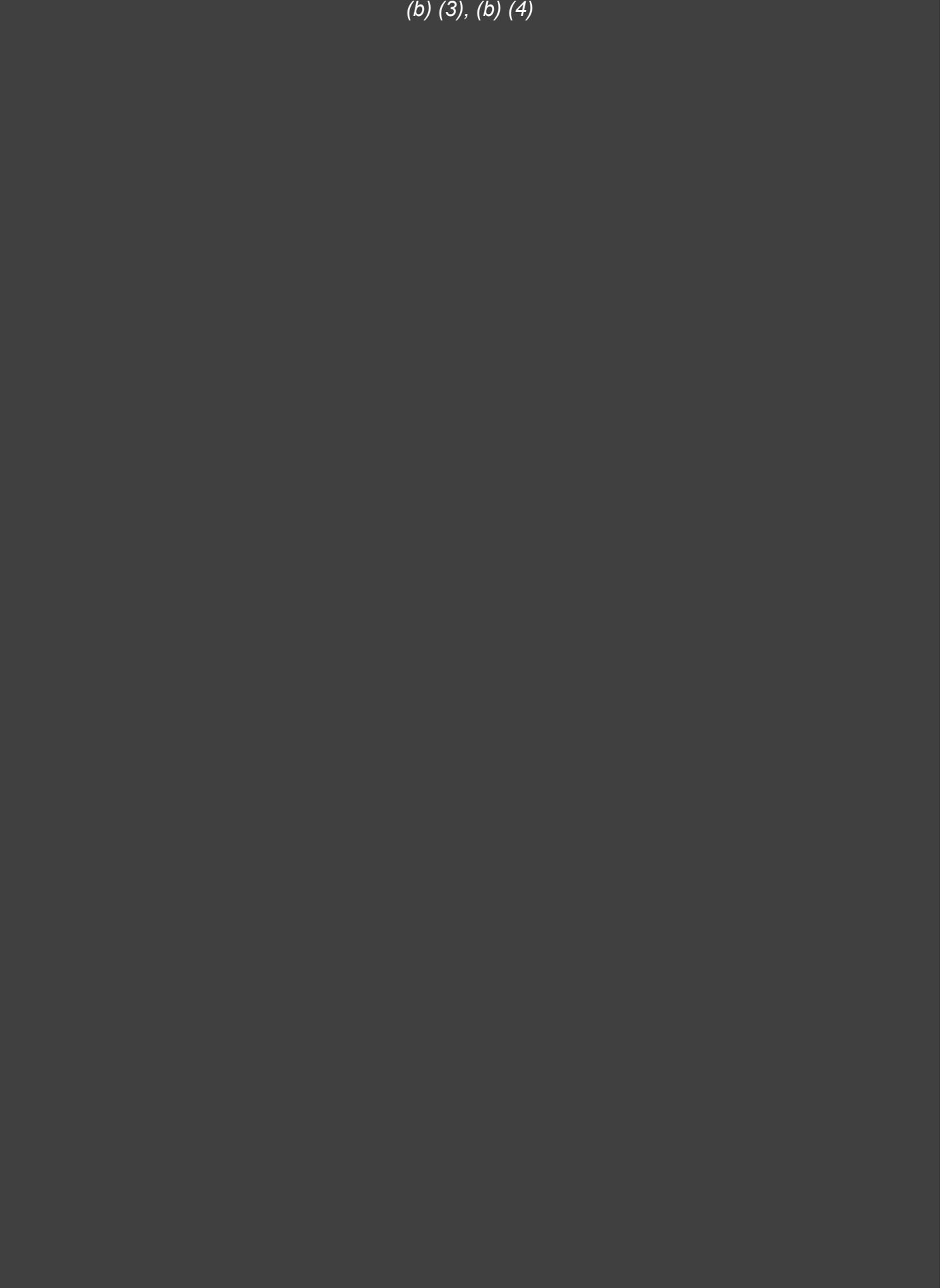
(b) (3), (b) (4)




(b) (3), (b) (4)




(b) (3), (b) (4)



(b) (3), (b) (4)



(b) (3), (b) (4)



Cisco Advanced Delivery Network Services (ADN)



...building the bridge of the future

Asset Lifecycle Analysis

Network assessments are designed and developed by CCIE/CCDP and ITIL qualified engineers. These assessments are designed to help you increase your network availability through the identification of leading-practice risks with specific recommendations to mitigate those risks based on your business and availability goals.

(b) (4)



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)